



Portsmouth, Virginia Police Department Department Organization

Data Storage Devices	ADM	31
Effective: 04.08.13	2	pages
Supersedes: New	CALEA: N/A	

APPROVED: Edward G. Hargis, Chief of Police

PURPOSE: To establish guidelines for the acceptable use of USB data storage devices, commonly referred to as flash drives, thumb drives, portable hard drives, etc., as a means of preventing unauthorized access to confidential police information and to prevent damage to department computer systems.

GUIDELINES:

Sensible use of department issued USB devices is permitted for business purposes.

This policy restricts the use of USB data storage devices to department issued devices only, unless otherwise authorized by an employee's supervisor. Supervisors can make exceptions to the use of non-department devices for investigative purposes (e.g., the victim of a crime presents video evidence of the incident to the investigator on a thumb drive) or in other very specific unique circumstances. Otherwise, the connection of privately owned USB data storage devices to department computers is not permitted.

It is each end user's responsibility and obligation to ensure that all data storage devices, where approved for use, are used only for their intended official purpose and that information contained or transmitted via these devices is protected from unauthorized use, copying or modification.

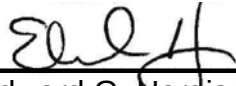
This policy should be considered an addition to City AP #1 section C and does not replace or otherwise remove department employee's responsibility to comply with City AP #1.

I. PROCEDURES:

- A. Issuance: Employees requiring a department issued USB data storage device will request issuance via email to the Technical Services Unit (TSU). TSU personnel will enter user information on the device for identification purposes and will set the device up before issuance.
- B. Asset Protection: The data and information stored and developed on computing assets of the Portsmouth Police Department must be protected against theft and data loss, at all times.
- C. Data/File Storage: Employees are required to store all City related electronic information and data on the City's network file servers. Issued USB data storage devices may be used for temporary and remote access to files, however work related files must not be stored on personally owned devices.
- D. Periodic Audit: USB data storage devices are subject to periodic internal audit and review and employees will be asked to justify any usage deemed inappropriate or excessive.

- E. Damage to systems and data: USB data storage devices with inappropriate software have the ability to cause potential damage to the confidentiality, integrity, and availability of any data and system files within the department.
- F. User Override: Department issued USB flash drives require a password to access the files, and all data on the drive will be deleted automatically after a specified number of unsuccessful access attempts. Users are not permitted to circumvent, subvert, or override any of the Department's security measures for USB devices.
- G. Loss of Device: If an employee loses a Department issued USB device, the employee shall immediately notify his or her supervisor who will, in turn, notify TSU via email. The employee will also complete a report for lost property.

APPROVED: _____


Edward G. Hargis, Chief of Police